IN THE CLAIMS

This listing of claims replaces all prior listings:

1. (currently amended) A computing environment, comprising:

an operating system;

a virtual machine operating on said operating system;

a first application operating on said virtual machine;

a second application operating on said virtual machine; and

a first firewall control block, wherein said first firewall control block defines access privileges of said first application with respect to said second application, and further defines the access privileges of said second application with respect to said first application,

wherein said first firewall control block includes a firewall control value and a firewall control indicator, the firewall control value including an application identifier data having a resource identifier and a proprietary identifier extension, the firewall control indicator being an indicator value represented by one or more bytes that indicate how the firewall control value should be interpreted with respect to access privileges of other applications, and

wherein when said firewall control indicator has a first indicator value, said first firewall control block compares said first application's proprietary identifier extension to said second application's proprietary identifier extension, and when said firewall control indicator has a second indicator value, said first firewall control block compares said first application's proprietary identifier extension and resource identifier to said second application's proprietary identifier extension and resource identifier.

2. (currently amended) A computing environment as recited in claim 1, wherein said computing environment further comprises:

a second firewall control block, wherein said second firewall control block defines access privileges of said second application with respect to said first application, and further defines ~~the~~ access privileges of said first application with respect to said second ~~first~~ application.

3. (original) A computing environment as recited in claim 1, wherein said first firewall control block defines access privileges of said first application with respect to any other application

in said computing environment, and further defines the access privileges of said any other application with respect to said first application.

4-5. (canceled).

6. (currently amended) A computing environment as recited in claim 1 [[4]], wherein said computing environment is a Java™ compliant computing environment, and wherein said first and second applications are Java™ compliant applets~~, and wherein said first firewall control value includes a RID~~.

7. (canceled).

8. (currently amended) A computing environment as recited in claim 1 [[4]], wherein said computing environment is a Java™ card compliant computing environment, and,

wherein said first firewall control block is implemented as in the run rime environment.

9. (currently amended) A mobile computing device, comprising:

an operating system;

a Java™ compliant virtual machine operating on said operating system;

a first Java™ compliant applet operating on said Java™ compliant virtual machine;

~~a~~ at least one other Java™ compliant applet operating on said ~~virtual machine~~ Java™ compliant virtual machine; and

a first firewall control block, wherein said first firewall control block defines access privileges of said first Java™ compliant applet with respect to the at least one other Java™ compliant applet operating on said Java™ compliant virtual machine, and further defines the access privileges of said at least one other Java™ compliant applet Java™ compliant applet with respect to said first Java™ compliant applet,

wherein said first firewall control block includes a firewall control value and a firewall control indicator, the firewall control value including an application identifier data having a resource identifier and a proprietary identifier extension, the firewall control indicator being an indicator value

represented by one or more bytes that indicate how the firewall control value should be interpreted with respect to access privileges of the at least one other Java™ compliant applet, and

wherein when said firewall control indicator has a first indicator value, said first firewall control block compares said first Java™ compliant applet's proprietary identifier extension to said at least one other Java™ compliant applet's proprietary identifier extension, and when said firewall control indicator has a second indicator value, said first firewall control block compares said first Java™ compliant applet's proprietary identifier extension and resource identifier to said at least one other Java™ compliant applet's proprietary identifier extension and resource identifier.

10. (original) A mobile computing device as recited in claim 9, wherein said mobile device is a Java™ compliant smart card.

11-14. (canceled).

15. (currently amended) A mobile computing device as recited in claim 10, wherein for a firewall control block is defined for every Java™ compliant applet.

16. (currently amended) A method of providing security for a Java™ compliant computing environment that includes a Java™ virtual machine and a plurality of Java™ compliant applets that operate on said Java™ virtual machine, said method comprising:

receiving a request from a first Java™ compliant applet operating on Java™ virtual machine to access a second Java™ compliant applet;

reading a firewall control block associated with said second Java™ compliant applet, said firewall control block including a firewall control value and a firewall control indicator, the firewall control value including an application identifier data having a resource identifier and a proprietary identifier extension, the firewall control indicator being an indicator value represented by one or more bytes that indicate how the firewall control value should be interpreted with respect to access privileges of the second Java™ compliant applet;

determining, based on said firewall control block, whether said first Java™ compliant applet should be allowed to access said second Java™ compliant applet by determining whether said firewall control value has a first indicator value or a second indicator value, wherein

when said firewall control indicator has a first indicator value, said firewall control block compares said first Java™ compliant applet's proprietary identifier extension to said second Java™ compliant applet's proprietary identifier extension, and

when said firewall control indicator has a second indicator value, said firewall control block compares said first Java™ compliant applet's proprietary identifier extension and resource identifier to said second Java™ compliant applet's proprietary identifier extension and resource identifier; and

allowing said first Java™ compliant applet to access said second Java™ compliant applet when said determining determines that access should be allowed.

17. (original) A method as recited in claim 16, wherein said method further comprises:

providing a reference to said first Java™ compliant applet with a reference to said second Java™ compliant when said determining determines that access should be allowed.

18. (currently amended) A method as recited in claim 16, wherein said providing of a reference comprises:

invoking a first method implemented that is implemented as a part of Java™ management environment or Java™ system ~~(or system)~~ environment; and

invoking a second method that is implemented as a Applet class, as a result of said invoking of the second method[[,]].

19. (original) A method as recited in claim 16, wherein said determining of whether said first Java™ compliant applet should be allowed to access said second Java™ compliant applet comprises:

reading a firewall control value; and

reading a firewall control indicator.

20. (currently amended) A method as recited in claim 16, wherein said determining of whether said first Java™ compliant applet should be allowed to access said second Java™ compliant applet comprises:

reading the first Java™ compliant applet's proprietary identifier extension ~~a first PID associated with said first Java™ compliant applet~~;

reading the second Java™ compliant applet's proprietary identifier extension ~~a second PID associated with said second Java™ compliant applet~~;

determining whether said first Java™ compliant applet's proprietary identifier extension ~~first PID~~ matches said second Java™ compliant applet's proprietary identifier extension ~~second PID~~; and

allowing access only when said determining determines that said first Java™ compliant applet's proprietary identifier extension ~~PID~~ matches said second Java™ compliant applet's proprietary identifier extension ~~PID~~.

21. (currently amended) A method as recited in claim 16, wherein said determining of whether said first Java™ compliant applet should be allowed to access said second Java™ compliant applet comprises:

reading the first Java™ compliant applet's proprietary identifier extension and resource identifier ~~a first PID associated with said first Java™ compliant applet~~;

reading the second Java™ compliant applet's proprietary identifier extension and resource identifier ~~a second PID associated with said second Java™ compliant applet~~;

determining whether said first Java™ compliant applet's proprietary identifier extension and resource identifier match ~~first PID matches~~ said second Java™ compliant applet's respective proprietary identifier extension and resource identifier ~~second PID~~; and

allowing access only when said determining determines that said first Java™ compliant applet's proprietary identifier extension and resource identifier match ~~PID matches~~ said second Java™ compliant applet's respective proprietary identifier extension and resource identifier ~~PID~~.

22. (currently amended) A computer readable media including computer program code for providing security for a computing environment, said computer readable media comprising:

computer program code for receiving a request from a first application to access a second application;

computer program code for reading a firewall control block associated with said second application, said firewall control block including a firewall control value and a firewall control indicator, the firewall control value including an application identifier data having a resource identifier and a proprietary identifier extension, the firewall control indicator being an indicator value represented by one or more bytes that indicate how the firewall control value should be interpreted with respect to access privileges of the second application;

determining, based on said firewall control block, whether said first application should be allowed to access said second application by determining whether said firewall control value has a first indicator value or a second indicator value, wherein

when said firewall control indicator has a first indicator value, said firewall control block compares said first application's proprietary identifier extension to said second application's proprietary identifier extension, and

when said firewall control indicator has a second indicator value, said firewall control block compares said first application's proprietary identifier extension and resource identifier to said second application's proprietary identifier extension and resource identifier; and

allowing said first application to access said second application when said determining determines that access should be allowed.